PERSONUPPGIFTSBITRÄDESAVTAL

Enligt artikel 28.3 i förordning 2016/679 (**GDPR**)

Den samarbetspartner som har ingått avtal med HPI Health Profile Institute AB om tillhandahållande av plattformen Plustoo

(**personuppgiftsansvarig**)

och

HPI Health Profile Institute AB, org. nr. 556714-5858
Magnus Ladulåsgatan 65, 118 27 Stockholm

(**personuppgiftsbiträde**)

var för sig kallade **part**; tillsammans **parterna**

HAR ENATS OM följande personuppgiftsbiträdesavtal (**avtalet**) för att uppfylla kraven i GDPR och för att säkerställa skyddet för den registrerades rättigheter.

1. Bakgrund

1.1 Avtalet anger den personuppgiftsansvariges och personuppgiftsbiträdes rättigheter och skyldigheter vid behandling av personuppgifter för den personuppgiftsansvariges räkning.

1.2 Avtalet har utformats för att säkerställa parternas efterlevnad av artikel 28.3 GDPR.

1.3 Parterna har ingått ett avtal om tillhandahållande av plattformen Plustoo (**huvudavtalet**). Plustoo är en digital plattform som bl.a. erbjuder samarbetspartner att genomföra tester, statistik, rapporter, nulägesanalyser och övrig administration av tjänsten. Syftet med Plustoo är att utveckla hälsa hos individer, grupper och organisationer (tillsammans, **tjänsterna**). Inom ramen för tillhandahållandet av tjänsterna kommer personuppgiftsbiträdet att behandla personuppgifter på personuppgiftsansvariges vägnar i enlighet med avtalet.

1.4 Avtalet har företräde framför alla liknande bestämmelser i huvudavtalet och andra eventuella avtal mellan parterna.

1.5 Till avtalet har det bifogats två bilagor som utgör en integrerad del av avtalet.

a) Bilaga A innehåller information om behandlingen av personuppgifter, inklusive syftet med behandlingen och dess art, typen av personuppgifter, kategorierna av registrerade och behandlingens varaktighet.

b) Bilaga B innehåller den personuppgiftsansvariges villkor för personuppgiftsbiträdet användning av underbiträden och en lista över underbiträden som är godkända av den personuppgiftsansvarige.

1.6 Avtalet fråntar inte personuppgiftsansvarige eller personuppgiftsbiträdet några skyldigheter enligt GDPR eller annan lagstiftning.

1.7 Avtalet är bara tillämpligt på de personuppgifter som personuppgiftsbiträdet behandlar enbart för den personuppgiftsansvariges räkning. I vissa fall kan personuppgiftsbiträdet av skäl som framgår av punkt 3.1 komma att behandla en viss typ av personuppgifter både för den personuppgiftsansvariges och för sin egen räkning. I så fall ska avtalets bestämmelser tillämpas enbart på sådan behandling som sker för den personuppgiftsansvariges räkning.

2. Den personuppgiftsansvariges rättigheter och skyldigheter

2.1 Den personuppgiftsansvarige ansvarar för att behandlingen av personuppgifter sker i enlighet med GDPR (se artikel 24 GDPR), andra tillämpliga dataskyddsbestämmelser och avtalet.

2.2 Den personuppgiftsansvarige har rätten och skyldigheten att fatta beslut om ändamål och medel för personuppgiftsbehandlingen.

2.3 Den personuppgiftsansvarige ska bland annat ansvara för att det finns en rättslig grund för den personuppgiftsbehandling som personuppgiftsbiträdet är instruerad att utföra.

3. Personuppgiftsbiträdet agerar i enlighet med instruktioner

3.1 Personuppgiftsbiträdet ska enbart behandla personuppgifter utifrån dokumenterade instruktioner från den personuppgiftsansvarige, såvida något annat inte följer av åtaganden i huvudavtalet, åtaganden gentemot registrerade eller följer av lagregler eller

andra regler som är tvingande för personuppgiftsbiträdet. Personuppgiftsbiträdets instruktioner specificeras i huvudavtalet samt i bilaga A.

3.2 Efterföljande instruktioner kan också ges av den personuppgiftsansvarige under tiden personuppgiftsbehandlingen pågår, men sådana instruktioner ska alltid dokumenteras och bevaras i skriftlig form, inklusive elektroniskt, tillsammans med avtalet.

3.3 Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige om en instruktion enligt personuppgiftsbiträdets mening är i strid med GDPR eller dataskyddsbestämmelser i annan EU-rätt eller medlemsstats nationella rätt, samt invänta instruktioner från den personuppgiftsansvarige innan personuppgiftsbehandlingen fortsätter.

4. Sekretess

4.1 Personuppgiftsbiträdet ska enbart ges tillgång till personuppgifter, som behandlas på personuppgiftsansvariges vägnar, till personer under personuppgiftsbiträdets kontroll, som har avgett ett sekretessåtagande eller som lyder under en lämplig lagstadgad tystnadsplikt, samt endast i den mån det behövs.

5. Säkerhet i samband med behandlingen

5.1 Artikel 32 GDPR föreskriver att med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personens rättigheter och friheter, ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

5.2 Den personuppgiftsansvarige ska utvärdera riskerna för fysiska personers rättigheter och friheter som är förknippade med behandlingen och genomföra åtgärder för att mildra dessa risker. Beroende på deras relevans kan åtgärderna omfatta följande:

a) pseudonymisering och kryptering av personuppgifter;

b) förmågan att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och -tjänsterna;

c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid händelse av en fysisk eller teknisk incident;

d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

5.3 Enligt artikel 32 GDPR ska personuppgiftsbiträdet också - oberoende av den personuppgiftsansvarige - utvärdera riskerna för fysiska personers rättigheter och friheter som är förknippade med behandlingen och genomföra åtgärder för att begränsa dessa risker. För detta ändamål ska den personuppgiftsansvarige förse personuppgiftsbiträdet med all information som krävs för att identifiera och mildra sådana risker.

5.4 Personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att säkerställa efterlevnaden av den personuppgiftsansvariges skyldigheter enligt artikel 32 GDPR, bland annat genom att förse den personuppgiftsansvarige med information om de tekniska och organisatoriska åtgärder som redan har genomförts av personuppgiftsbiträdet enligt artikel 32 GDPR tillsammans med all annan information

som är nödvändig för att den personuppgiftsansvarige ska uppfylla sina skyldigheter enligt artikel 32 GDPR.

5.5 Om begränsningen av de identifierade riskerna kräver ytterligare åtgärder, ska den personuppgiftsansvarige specificera dessa ytterligare åtgärder.

6. Användning av underbiträde

6.1 Personuppgiftsbiträdet har den personuppgiftsansvariges allmänna godkännande att använda underbiträden. Personuppgiftsbiträdet ska informera den personuppgiftsansvarige om alla avsedda ändringar som rör tillägg eller utbyte av underbiträden och därigenom ge den personuppgiftsansvarige möjlighet att invända mot sådana förändringar innan underbiträdet anlitas. En lista över redan godkända underbiträden finns i bilaga B.

6.2 Om personuppgiftsbiträdet anlitar ett underbiträde för att utföra specifika behandlingar på den personuppgiftsansvariges vägnar, ska personuppgiftsbiträdet vara ansvarig för att ålägga underbiträdet samma skyldigheter avseende dataskydd som anges i detta avtal, genom ett kontrakt eller annan rättslig handling. Där ska det uttryckligen ges tillräckliga garantier för att underbiträdet genomför lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen kommer att uppfylla kraven i avtalet och GDPR. Personuppgiftsbiträdet är därför ansvarig för att kräva att underbiträdet åtminstone uppfyller de skyldigheter som personuppgiftsbiträdet är föremål för enligt avtalet och GDPR.

6.3 Om underbiträdet inte uppfyller sina skyldigheter avseende dataskydd ska personuppgiftsbiträdet förbli fullt ansvarig i förhållande till den personuppgiftsansvarige vad gäller uppfyllandet av underbiträdets skyldigheter. Detta påverkar inte de registrerades rättigheter, särskilt artikel 79 och 82 i GDPR, i förhållande till den personuppgiftsansvarige och personuppgiftsbiträdet, inklusive underbiträdet.

7. Överföring av personuppgifter till tredjeland

7.1 Personuppgiftsbiträdets eventuella överföring av personuppgifter till tredje land ska endast ske på grundval av dokumenterade instruktioner från den personuppgiftsansvarige och ska alltid ske i enlighet med GDPR, kapitel V.

7.2 Vid överföringar till tredjeland, som personuppgiftsbiträdet inte har fått i uppdrag att utföra av den personuppgiftsansvarige, men som krävs enligt EU-rätten eller en medlemsstats lag som personuppgiftsbiträdet är föremål för, ska personuppgiftsbiträdet informera den personuppgiftsansvarige såvida inte denna lag förbjuder sådan information på grund av viktiga skäl av allmänt intresse.

7.3 Utan dokumenterade instruktioner från den personuppgiftsansvarige får personuppgiftsbiträdet därför inte inom ramen för avtalet:

a) överföra personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredjeland,

b) överföra behandlingen av personuppgifter till ett underbiträde i ett tredjeland, eller

c) låta personuppgifter behandlas av personuppgiftsbiträdet i ett tredjeland.

7.4 Detta avtal ska inte förväxlas med standardavtalsklausuler som nämns i artikel 46.2 c-d GDPR, och detta avtal kan inte utgöra grund för överföring av personuppgifter som behandlas i GDPR:s kapitel V.

8. Assistans till den personuppgiftsansvarige

8.1 Personuppgiftsbiträdet bistår, på begäran av den personuppgiftsansvarige och med beaktande av behandlingens art, i mån detta är möjligt, den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, med fullgörandet av den personuppgiftsansvariges skyldigheter att efterkomma en begäran om utövande av den registrerades rättigheter enligt kapitel III GDPR, inklusive, men inte begränsat till, rätten till information, rätten till tillgång, rätten att radera, rätten till begränsning av behandlingen, rätten till dataöverföring och rätten att invända.

8.2 Personuppgiftsbiträdet ska dessutom, med beaktande av behandlingens art och den information som är tillgänglig för personuppgiftsbiträdet, hjälpa den personuppgiftsansvarige att säkerställa efterlevnad av:

a) den personuppgiftsansvariges skyldighet att utan onödigt dröjsmål och, om möjligt, senast 72 timmar efter att ha fått kännedom om det, anmäla personuppgiftsincidenter till den behöriga tillsynsmyndigheten (DPA), dvs. Integritetsskyddsmyndigheten, såvida det inte är osannolikt att personuppgiftsincidenten leder till en risk för fysiska personers rättigheter och friheter;

b) den personuppgiftsansvariges skyldighet att utan onödigt dröjsmål underrätta berörda registrerade om personuppgiftsincidenten, när personuppgiftsincidenten sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter;

c) den personuppgiftsansvariges skyldighet att göra en bedömning av planerade personuppgiftsbehandlingars inverkan på skyddet av personuppgifter (en konsekvensbedömning);

d) den personuppgiftsansvariges skyldighet att konsultera DPA innan behandlingen inleds, om en konsekvensbedömning visar att behandlingen skulle resultera i en hög risk då tillräckliga åtgärder för att mildra risken inte vidtagits.

9. Underrättelse om personuppgiftsincident

9.1 Vid en personuppgiftsincident ska personuppgiftsbiträdet utan onödigt dröjsmål och, om möjligt, inom fyrtioåtta (48) timmar efter att ha fått kännedom om denna, meddela den personuppgiftsansvarige om personuppgiftsincidenten.

9.2 Personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att anmäla personuppgiftsincidenten till DPA, vilket innebär att personuppgiftsbiträdet är skyldig att bistå med att få den information som ska anges i den personuppgiftsansvariges anmälan till DPA:

a) personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

b) de sannolika konsekvenserna av personuppgiftsincidenten,

c) de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att begränsa dess potentiella negativa effekter.

10. Radering och återlämnande av information

10.1 Vid upphörande av tillhandahållandet av tjänsterna relaterade till personuppgiftsbehandlingen ska personuppgiftsbiträdet, i enlighet med personuppgiftsansvariges instruktioner, antingen

a) radera alla personuppgifter som behandlas på personuppgiftsansvariges vägnar och intyga att personuppgiftsbiträdet har gjort det, eller
b) anonymisera alla personuppgifter som behandlas på personuppgiftsansvariges vägnar och intyga att personuppgiftsbiträdet har gjort det, eller
c) återlämna alla personuppgifter till den personuppgiftsansvarige och radera befintliga kopior såvida inte tillämplig lag (såsom svensk bokföringslag (1999: 1078) eller svensk penningtvätt och finansiering av terrorismfinansiering (2017: 630) kräver lagring av personuppgifter).

10.2 Om personuppgansvarige önskar att personuppgiftsbiträdet återlämnar alla personuppgifter, ska personuppgifterna återlämnas i ett överenskommet tekniskt format och mot arbete enligt timtaxa.

11. Granskning och inspektion

11.1 Den personuppgiftsansvarige har rätt att, i den omfattning som krävs enligt GDPR, antingen på egen hand eller med hjälp av tredje part, på det sätt som är lämpligt, granska personuppgiftsbiträdets verksamhet och databehandlingsutrustning i syfte att säkerställa att personuppgiftsbiträdet, samt eventuella underbiträden, uppfyller sina åtaganden enligt artikel 28 GDPR och avtalet. Eventuellt besök i personuppgiftsbiträdets lokaler ska ske under normal kontorstid och med skäligt varsel. Med skäligt varsel avses normalt tio (10) arbetsdagar.

11.2 Personuppgiftsbiträdet åtar sig att tillhandahålla den information och/eller den assistans som den personuppgiftsansvarige skäligen kan begära i samband med granskning enligt punkten 11.1. Detta ska ske på den personuppgiftsansvariges bekostnad. Personuppgiftsbiträdet ska tillåta de inspektioner som DPA kan kräva för säkerställandet av en korrekt behandling av personuppgifterna som omfattas av avtalet och följa eventuella beslut av DPA om behandling av sådana personuppgifter. Även detta ska ske på den personuppgiftsansvariges bekostnad.

12. Parternas avtal om andra förhållanden

12.1 Parterna kan avtala om andra bestämmelser angående tjänsterna relaterade till personuppgiftsbehandlingen om exempelvis ersättningsansvar, så länge som dessa andra bestämmelser inte direkt eller indirekt strider mot avtalet eller begränsar den registrerades grundläggande rättigheter och friheter som följer av GDPR.

12.2 Skulle en registrerad, tillsynsmyndighet eller annan tredje part göra anspråk, väcka talan eller ålägga en sanktion mot den personuppgiftsansvarige som grundar sig på att personuppgiftsbiträdet har försummat att fullgöra sina skyldigheter enligt tillämpliga dataskyddsbestämmelser, avtalet och/eller dokumenterade instruktioner från den

personuppgiftsansvarige, ska personuppgiftsbiträdet ersätta och hålla den personuppgiftsansvarige skadeslös för förlust eller kostnad, inklusive sanktionsavgifter.

12.3 Ingen part har rätt att helt eller delvis överlåta sina skyldigheter eller rättigheter enligt avtalet till en tredje part.

13. Ikraftträdande, upphörande och ändringar

13.1 Avtalet gäller från det datum parterna ingick huvudavtalet.

13.2 Vardera parten har rätt att begära att avtalet omförhandlas om det krävs på grund av ändrad lag eller myndighetsbeslut eller om avtalet helt eller delvis skulle vara ogiltigt.

13.3 Avtalet ska gälla tills det senare av (a) upphörandet av tillhandahållandet av tjänsterna för behandling av personuppgifter (b) upphörandet av huvudavtalet och (c) fullgörandet av personuppgiftsbiträdets skyldigheter enligt avsnitt 10 ovan.

13.4 Under den tid som tillhandahållandet av tjänsterna för behandling av personuppgifter kan avtalet inte sägas upp om inte ett annat avtal som reglerar tillhandahållandet av tjänster för behandling av personuppgifter har avtalats mellan parterna.

13.5 Eventuella ändringar eller ändringar av avtalet ska göras skriftligen och undertecknas av vederbörligen bemyndigade företrädare för båda parter.

14. Kontaktpersoner/kontaktuppgifter till personuppgiftsansvarig och personuppgiftsbiträdet

14.1 Parterna kan tillse att parterna har uppdaterade kontaktuppgifter till varandra.

15. Tillämplig lag och tvistlösning

15.1 Avtalet och all behandling av personuppgifter som sker enligt avtalet regleras av svensk lag, med undantag för tillämpliga regler om lagval. Varje tvist angående tolkningen eller tillämpningen av avtalet ska avgöras enligt bestämmelserna om tvistlösning i huvudavtalet.

_____

BILAGA A - INFORMATION OM TYP AV BEHANDLING

A.1. Syftet med personuppgiftsbiträdets behandling av personuppgifter på uppgiftsansvariges vägnar är:

Att administrera och tillhandahålla de tjänster som omfattas av huvudavtalet.

A.2. Personuppgiftsbiträdets behandling av personuppgifter på uppgiftsansvarigens vägnar ska främst avse (behandlingens art):

Att samla in, organisera, strukturera, analysera, lagra, bearbeta, använda, utlämna genom överföring, anonymisera och radera data om användarna av tjänsten som omfattas av huvudavtalet.

A.3. Behandlingen inkluderar följande typer av personuppgifter om registrerade:

- Namn
- Personnummer
- Mailadress
- Arbetsgivare
- Yrke
- Uppgifter om hälsa
- Uppgifter om arbetsmiljö

A.4. Behandlingen inkluderar följande kategorier av registrerade:

Parts medarbetare samt kundmedarbetare och/eller andra privatpersoner som använder eller har tillgång till tjänsten.

A.5. Personuppgiftsbiträdets behandling av personuppgifter på den uppgiftsansvariges vägnar kan utföras när avtalet börjar. Behandlingen har följande varaktighet:

Under hela huvudavtalets giltighet och därefter i enlighet med den personuppgiftsansvariges instruktioner enligt punkt 10 i detta avtal.

BILAGA B - GODKÄNDA UNDERBITRÄDEN

B.1. Godkända underbiträden
Den personuppgiftsansvarige godkänner de underbiträden som, vid datumet för huvudavtalets ingående, framgår på följande länk: https://www.hpi-plustoo.com/villkor.

Underbiträden kommer vid var tid framgå på ovan länk. Den personuppgiftsansvarige får information om eventuella ändringar av underbiträden genom att ta del av den information som finns på ovan länk.